|  |  |
| --- | --- |
|  | Si rempli, min.: INTERNE |

|  |
| --- |
|  |

P042-Hi01 - Concept de sécurité de l’information et de protection des données (concept SIPD)

<Nom du projet / nom de l’objet à protéger>

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Classification | INTERNE, CONFIDENTIEL, SECRET |
| Statut | En cours d’élaboration, en cours de vérification, terminé/approuvé |
| Numéro du projet |  |
| Chef de projet (CP BP) |  |
| Version | Du template V4.4 |
| Date |  |
| Mandant |  |
| Auteur(s) |  |

Suivi des modifications

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description, remarque | Nom |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribution

|  |  |  |
| --- | --- | --- |
| Fonction | Nom | Département / office |
| DSIO |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Évaluation du document après les phases de projet

Les tableaux indiquant les personnes qui examinent (confirment) les différentes phases peu-vent être complétés par autant de noms que souhaité.

Initialisation – avant la libération du projet

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Fonction | Nom | Date |
|  | Resp. SIPD |  |  |
| DSIO |  |  |
|  |  |  |

Conception – avant la libération de phases

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Fonction | Nom | Date |
|  | Resp. SIPD |  |  |
| DSIO |  |  |
|  |  |  |

Réalisation – avant la libération de phases

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Fonction | Nom | Date |
|  | Resp. SIPD |  |  |
| DSIO |  |  |
|  |  |  |

Déploiement – avant la mise en service

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Fonction | Nom | Date |
|  | Resp. SIPD |  |  |
| DSIO |  |  |
|  |  |  |

Table des matières

1 Remarques générales 5

1.1 Description 5

1.2 But du document 5

1.3 Validité du document 5

2 Résumé 6

2.1 Généralités 6

2.2 Résumé des risques résiduels 6

2.3 Remarques finales 6

2.4 Approbation 7

3 Liste des documents relatifs à la sécurité 8

4 Classification d’après le P041 - Analyse des besoins de protection 9

5 Description du système du point de vue de la sécurité 9

5.1 Interlocuteurs et responsabilités 9

5.2 Description du système global 9

5.3 Description des données à traiter 10

5.4 Esquisse de l’architecture et matrice de communication 10

5.5 Description de la technologie sous-jacente 11

6 Analyse des risques et mesures de protection 12

6.1 Risques résiduels 12

7 Rétablissement des activités 13

8 Respect, contrôle et approbation des mesures de protection 13

8.1 Contrôle de la réception du système 14

9 Mise hors service 14

10 Abréviations 15

11 Annexe 16

# Remarques générales

**Remarques sur la façon de remplir le document**

Le processus de sécurité vise la prise en compte de la sécurité informatique dans les projets ainsi que lors de l’introduction et de l’utilisation de moyens informatiques. Pour garantir le respect de ce processus, des documentations spécifiques sont exigées. Le NCSC fournit des modèles à cet effet. Il est possible d’adapter ces modèles (notamment le contenu) à ses propres besoins et objectifs. Ces modèles doivent être considérés comme des outils aidant à respecter toutes les directives de sécurité. Ils servent de liste de contrôle pour tenir compte de tous les aspects concernant la sécurité.

* Le texte en noir correspond à des blocs de texte conformes aux prescriptions légales. Ceux-ci doivent, pour autant qu'ils soient cohérents, être repris et ne pas être modifiés.
* Le texte en bleu sert d’aide pour remplir le document. Il doit être supprimé après qu’un texte concret, spécifique et adapté au projet a été inséré.
* Le texte en rouge correspond à des indications ou à des questions importantes, qu’il faut clarifier ou décrire concrètement.
* Si la classification d’après le P041 - Analyse des besoins de protection (chap. 4) ne révèle pas de besoin de protection accru, mais que l’on doit ou souhaite tout de même rédiger un concept SIPD (par ex. une conséquence ou une exception à la protection informatique de base), alors l’analyse des risques (chap. 6) peut être omise.

## Description

Description de l’objet à protéger

## But du document

Le concept SIPD définit les indications nécessaires pour le maintien et l’amélioration de la sécurité de l’information et de la protection des données.

Il récapitule les aspects de la sécurité de l’information et de la protection des données dans le projet.

L’art. 4, al. 1, et l’art. 14, al. 3, de l’ordonnance sur les cyberrisques (OPCy) permettent de définir une partie des bases sur lesquelles devrait reposer tout projet informatique.

Toutes les mesures de sécurité applicables aux différents objets informatiques à protéger doivent être documentées sous une forme actualisée (selon l’art. 14, al. 3, OPCy). C’est notamment l’objectif du concept SIPD (art. 14*d,* al. 1, OPCy).

## Validité du document

Le concept SIPD est valable au maximum 5 ans.

# Résumé

Le résumé doit être rédigé de façon à ce que même les personnes ne possèdant pas de connaissances techniques approfondies puissent le comprendre.

## Généralités

Résumé des indications figurant dans le document et concernant l’analyse des risques effectuée, la sécurité de l’information et la protection des données. Il donne une image du potentiel de risque du système examiné.

## Résumé des risques résiduels

Un résumé et une évaluation des risques résiduels doivent être effectués selon le chapitre 6.1. La décision d’assumer ou non les risques résiduels appartient au responsable de l’unité administrative compétente.

## Remarques finales

Remarques finales et conclusions importantes relatives à l’objet informatique à protéger.

## Approbation

Les signatures relatives à l’approbation et à l’acceptation des risques résiduels doivent être apposées avant la mise en service.

Par sa signature, le DSIO confirme avoir examiné le concept SIPD. Il a en particulier vérifié que le document est rempli de manière complète, que toutes les mesures sont documentées. Il a examiné les informations d'un œil critique et a vérifié qu'elles sont cohérentes et applicables à l'objet informatique à protéger.

Par leur signature, le mandant et le responsable des processus d’affaires approuvent le concept SIPD.

Le responsable de l’unité administrative compétente décide d’assumer ou non les risques résiduels connus[[1]](#footnote-1). Selon les dispositions internes à l’office, ce document peut également être signé par un autre membre de la direction.

|  |  |
| --- | --- |
| Date / nom / signature **DSIO**: | …………………………………………………...…... |
| Date / nom / signature **Mandant**:  | …………………………………………………...…... |
| Date / nom / signature **Responsable du processus d’affaires**:  | …………………………………………………...…... |
| Date / nom / signature **Responsable de l’unité administrative ou membre de la direction**:  | …………………………………………………...…... |

**D’autres signatures peuvent être ajoutées (par ex. celle du responsable chez le FP).**

**Les signatures peuvent aussi être apposées sous forme électronique (dans un PDF).**

# Liste des documents relatifs à la sécurité

Il s’agit de citer les bases légales sur lesquelles s'appuie le projet informatique (à réaliser) prend appui. Ce travail s’effectue de préférence en collaboration avec le service juridique de l’unité administrative ou du département.

Un modèle d’analyse des bases légales est disponible à l’adresse suivante: <http://www.hermes.admin.ch/onlinepublikation/index.xhtml?element=ergebnis_rechtsgrundlagenanalyse.html>.

Certains risques ou dangers peuvent parfois être couverts par des concepts généraux de sécurité ou par des SLA. Ces documents sont énumérés ci-dessous.

La liste doit être complétée par les documents propres au département et/ou à l’office.

|  |  |
| --- | --- |
| Type de document | Titre |
| Loi | [Loi fédérale sur la protection des données (LPD; RS 235.1)](https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html) |
|  | [Loi fédérale sur l’archivage (LAr; RS 152.1)](https://www.admin.ch/opc/fr/classified-compilation/19994756/index.html)  |
|  |  |
| Ordonnance | [Ordonnance sur](https://www.admin.ch/opc/fr/classified-compilation/20081009/index.html) les cyberrisques (OPCy; RS [120.73](https://www.fedlex.admin.ch/eli/cc/2020/416/fr)) |
|  | [Ordonnance concernant la protection des informations (OPrI; RS 510.411)](https://www.admin.ch/opc/fr/classified-compilation/20070574/index.html)  |
|  | [Ordonnance relative à la loi fédérale sur la protection des données (OLPD; RS 235.11)](https://www.admin.ch/opc/fr/classified-compilation/19930159/index.html) |
|  | Ordonnance sur la transformation numérique et l’informatique (OTNI; [172.010.58](https://www.fedlex.admin.ch/eli/cc/2020/988/fr)) |
|  | [Ordonnance sur le traitement des données personnelles liées à l’utilisation de l’infrastructure électronique de la Confédération](https://www.admin.ch/opc/fr/classified-compilation/20111415/index.html) (RS 172.010.442) |
|  |  |
| Directive |  |
|  |  |
| Stratégie | [Stratégie informatique de la Confédération](https://www.isb.admin.ch/isb/fr/home/themen/strategie_planung/ikt-strategie_bund_2016-2019.html) |
|  |  |
| Méthode | [HERMES – La méthode suisse de gestion de projet](http://www.hermes.admin.ch/) |
|  |  |
| Concepts généraux de sécurité |  |
| SLA |  |
|  |  |
| Autres | 🡺 À compléter par l’auteur |

#

# Classification d’après le P041 - Analyse des besoins de protection

La classification de l’objet informatique à protéger doit être réalisée selon l’analyse des besoins de protection ([P041 - Analyse des besoins de protection](https://intranet.ncsc.admin.ch/ncscintra/fr/home/vorgaben-hilfsmittel/sicherheitsverfahren/beurteilung-schutzbedarf.html))[[2]](#footnote-2).

Les évaluations effectuées lors de l’analyse des besoins de protection permettent aussi d’estimer les éventuelles conséquences financières des besoins en matière de sécurité et de les décrire dans le présent document.

# Description du système du point de vue de lasécurité

Description condensée des éléments relatifs à la sécurité du système, des applications, des fichiers de données disponibles et traités ainsi que des processus qui s’y rapportent.

##  Interlocuteurs et responsabilités

|  |  |
| --- | --- |
| Qui | Nom |
| Responsable de l’application |  |
| Propriétaire des données |  |
| Exploitant du système FP |  |
| Chef de projet BP |  |
| Interlocuteur auprès du FP |  |
| DSID |  |
| DSIO |  |
| CPDO |  |
| Cercle d’utilisateurs |  |
| Autres services |  |

##  Description du système global

Description des fonctionnalités ayant un impact sur la sécurité, telles que les répartitions de rôles, la méthode d’authentification, la sauvegarde, les processus de support et de maintenance (év. à distance), les SLA, etc.

Il est aussi possible de faire référence aux documents correspondants (nom, date de création, lieu d’enregistrement, etc.). La description doit être complète et pouvoir être comprise par des personnes non impliquées.

##  Description des données à traiter

Description des données et des structures (par ex. base de données utilisée).

Les questions suivantes doivent être clarifiées et exposées lors du traitement de données personnelles:

* Fichier de données annoncé au PFPDT ?

Il s’agit de déterminer si le traitement des données satisfait aux dispositions de la loi fédérale sur la protection des données. Il convient notamment de vérifier si un fichier de données doit être annoncé au PFPDT.

* Un règlement de traitement doit-il être établi? Consultez à cet égard le [Règlement de traitement](https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/prozesse-methoden/p042-informationssicherheits-und-datenschutzkonzept_ISDS.html) ou l’ordonnance relative à la loi fédérale sur la protection des données (OLPD) ainsi que le document disponible sous le lien suivant : [Guide relatif aux mesures techniques et organisationnelles de la protection des données](https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/guides/mesures-techniques-et-organisationnelles-de-la-protection-des-do.html)
Si oui, renvoyez au document correspondant.
* Existe-t-il une base légale relative au traitement électronique des données?
* Les données doivent-elles être mises à la disposition des Archives fédérales sous forme électronique ?
* Si les informations sont classifiées, l’OPrI et les [prescriptions de traitement](https://intranet.vbs.admin.ch/de/wissen/integrale-sicherheit/grundlagen-vorgaben-internationales/kischb.detail.document.html/vbs-intranet/de/documents/integrale-sicherheit/grundlagen-vorgaben-internationales/kischb/Bearbeitungsweisungend.pdf.html) doivent être respectées (seulement sur l’intranet et en allemand).
* Si l’objet à protéger est pertinent pour le processus d’audit GRAES, il faut renvoyer au document correspondant.

## Esquisse de l’architecture et matrice de communication

Insérer ici une esquisse de l’architecture et une matrice de communication ou renvoyer au document correspondant tenu à jour.

 



## Description de la technologie sous-jacente

Description des techniques utilisées, telles que plate-forme de serveurs, système(s) d’exploitation, environnement système, réseaux utilisés, fonctions cryptographiques, etc. Ces techniques doivent être décrites de manière complète et pouvoir être comprises aussi par des personnes non impliquées. Ou renvoi au document correspondant tenu à jour

# Analyse des risques et mesures de protection

Description des facteurs de risques pertinents (disponibilité, confidentialité, intégrité et traçabilité), liste et évaluation des risques, y compris risques provenant d’une potentielle pertinence pour le processus d’audit GRAES.

L’[analyse des risques](https://intranet.ncsc.admin.ch/ncscintra/fr/home/vorgaben-hilfsmittel/sicherheitsverfahren/erhoehter-schutz.html) détaillée doit être effectuée à l’aide du fichier Excel faisant partie du concept. Des remarques sur la façon de le remplir se trouvent dans le document Excel.

Résultats de l’analyse des risques:

Les feuilles «Disponibilité», «Confidentialité», «Intégrité», «Traçabilité», «Synthèse» et «Synthèse Radar» sont des graphiques desquels ressort la catégorie du risque évalué.

* Vert: ces risques sont soit inhérents (à l’objet à protéger en tant que tel) ou peuvent être négligés. Ils doivent pouvoir être réduits par des mesures simples.
* Jaune: ces risques ont des conséquences considérables et doivent donc être réduits.
* Rouge: ces risques sérieux ont des conséquences critiques à catastrophiques. Ils doivent impérativement être réduits.

🡺 Les risques qui ne peuvent pas être traités (réduits) ou qui ne peuvent l’être que de manière insuffisante (surlignés en rouge ou en jaune dans la matrice des risques résiduels) doivent être inscrits dans le concept SIPD (chap. 6.1). Il faut les indiquer et informer par écrit le mandant et les responsables des processus d’affaires. La décision d’assumer ou non les risques résiduels connus appartient au responsable de l’unité administrative compétente.

Les risques résiduels doivent aussi être récapitulés brièvement dans le résumé (chap. 2.2).

## Risques résiduels

Il faut insérer ici la grille «Matrice des risques résiduels» provenant de l’analyse des risques.



Il faut fournir dans le tableau qui suit une justification des risques résiduels (surlignés en rouge et en jaune).

|  |  |  |
| --- | --- | --- |
| **N°** | **Risque** | **Justification** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Rétablissement des activités

Un plan d’urgence doit être établi pour les objets à protéger qui soutiennent des processus d’affaires critiques.

Il décrit la planification des cas d’urgence et la prévention des catastrophes de l’objet informatique à protéger afin de garantir le maintien et le rétablissement des activités dans les situations extraordinaires. Une aide est disponible dans le document «P042-Hi03 - Plan d’urgence»[[3]](#footnote-3).

Dans tous les cas, il faut renvoyer aux documents de la BCM au niveau de l’office.

# Respect, contrôle et approbation des mesures de protection

Description du règlement d’exécution des révisions et contrôles, annoncés ou non, des activités de sécurité de l’information dans le projet, puis dans l’exploitation.

## Contrôle de la réception du système

🡺 Les systèmes, nouveaux ou actualisés, doivent faire l’objet d’un examen et d’un contrôle poussés lors du processus de développement, comprenant la préparation d’une planification approfondie des activités, d’informations sur les tests internes et des dépenses attendues dans différentes conditions. Tout comme pour les projets de développement, ce type d’exa-mens doit tout d’abord être effectué par l’équipe de développement. Ensuite, des examens de réception indépendants doivent être entrepris (pour les projets de développement internes comme pour les projets externalisés) afin de vérifier que le système fonctionne comme prévu (et uniquement comme prévu, voir ISO/IEC 27002:2013, chapitre 14.1.1 et 14.1.2). La portée de ces examens doit correspondre à l’importance et à la qualité du système.

Résumé des audits effectués (qui, quand, quoi, résultat).

# Mise hors service

Description des points à respecter lors de la mise hors service.

# Abréviations

**Définitions, acronymes et abréviations**

|  |  |
| --- | --- |
| Acronymes / Abréviations | Contexte |
| BCM | Gestion de la continuité des activités |
| Concept SIPD | Concept de sécurité de l’information et de protection des données  |
| CPDO | Conseiller à la protection des données de l’organisation |
| DSID | Délégué à la sécurité informatique du département  |
| DSIO | Délégué à la sécurité informatique de l’unité d’organisation  |
| GRAES | Méthode de gestion des risques visant à réduire les activités d’espionnage de services de renseignement |
| LPD | Loi fédérale du 19 juin 1992 sur la protection des données |
| NCSC | Centre national pour la cybersécurité |
| OLPD | Ordonnance relative à la loi fédérale sur la protection des données |
| PFPDT | Préposé fédéral à la protection des données et à la transparence |
| RA | Responsable d’application |
| RSIPD | Responsable de la sécurité de l’information et de la protection des données dans le cadre du projet, selon HERMES |
| SLA | Service Level Agreement |
| RS | Responsable système |

# Annexe

Ajouter ici les documents complémentaires correspondants tels que, au minimum:

* P041-Hi01 - Analyse des besoins de protection
* P042-Hi02 - Analyse des risques
1. Art. 14*d*, al. 3, OPCy [↑](#footnote-ref-1)
2. [intranet.ncsc.admin.ch](https://intranet.ncsc.admin.ch/ncscintra/fr/home/vorgaben-hilfsmittel/sicherheitsverfahren/beurteilung-schutzbedarf.html) > Directives informatiques & outils > Procédures de sécurité > Appréciation des besoins de protection > P041 - Analyse des besoins de protection [↑](#footnote-ref-2)
3. [intranet.ncsc.admin.ch](https://intranet.ncsc.admin.ch/ncscintra/fr/home/vorgaben-hilfsmittel/sicherheitsverfahren/erhoehter-schutz.html) > Directives informatiques & outils > Procédures de sécurité > Protection élevée > P042 - Concept de la sécurité de l’information et de protection des données (SIPD) [↑](#footnote-ref-3)